Shubham Paikrao

🎯 Malware / Ransomware

🚨 1. Identification

Task	Details
Detection Sources	- EDR/AV alerts - SIEM alerts - User reports - Abnormal network activity
Indicators of Compromise (IOCs)	- Unusual file extensions (e.g., .locked, .crypt) - Ransom note files - Suspicious processes or network traffic - Locked-out users - High CPU usage or unknown processes - Disabled antivirus or backups
Initial Triage	- Confirm infection - Determine scope (how many endpoints, systems, users?) - Network segment - Sensitive data exposure - Document initial findings

---

✅ 2. Immediate Actions & 🧯 Containment

Short Term (0-1 hr)

- Isolate infected endpoints from the network → Use the EDR console or physically unplug.
- Disable compromised accounts → Lock AD credentials or revoke tokens.
- Block known malicious IPs/domains → VLAN segmentation or firewall blocks.
- Stop spreading by disabling shared drives → Prevent lateral movement and propagation

Long term (1-24 hr)

- Apply patches/updates → Especially if exploited in this attack.
- Tighten endpoint controls → Ensure detection of current malware strain.
- Force password changes where needed → Force a change for users with compromised devices.
- Restrict remote access → Disable RDP unless necessary.

🛠️ 3. Eradication

- Malware Removal → Use EDR tools or forensic imaging, or bootable AV tools to scan and remove malware or reimage the system if necessary.
- Root Cause Analysis → How did it get in? (Phishing, USB, drive-by download?)
- IOC Search → What vulnerabilities were exploited?
- Persistence → Search all endpoints and logs for the presence of IOCs across the organization.
- Removal → Check for startup registry entries, scheduled tasks, WMI scripts, or malicious services.
- Validate with Forensics → Perform memory and disk forensics on at least one infected device. Save forensic images before reimaging.

🩺 4. Recovery

Task	Details
System Restoration	Use clean backups to restore affected endpoints. Ensure no IOCs exist in the restored environment.
Rejoin Network	Reconnect endpoints only after complete scanning and validation.
Validation	Ensure all malware is removed
Monitor Post Recovery	Enable enhanced logging. Monitor for repeat infections or anomalies.
Business Resumption	Provide regular updates to internal teams, executives, and if necessary, regulators.

📝 5. Reporting & Documentation

📂 5.1 Evidence & Artifacts Collected

- Memory dumps (e.g., .vmem, .raw)
- Disk images
- Ransom notes
- Malware samples
- Logs: Windows Event Logs, EDR telemetry, firewall logs, DNS logs
- Email headers (if phishing was involved)

📜 5.2 Timeline of Events

- Time
- Action taken

📬 5.3 Notifications & Communications

- Full summary
- What went well / What didn't
- Action items with owners and deadlines
- Recommendations for improving detection, response, and resilience
- Date for follow-up readiness test or tabletop exercise

🔁 6. Lessons Learned / Review

Task	Details
Post-Incident Review	-Within 72 hours of the incident being closed, conduct a meeting with stakeholders.
Documentation	- Incident timeline - Actions taken - What worked/failed
Policy & Process Update	- Improve security controls - Update training, tools, and playbooks based on findings

---

✅ Quick Checklist for On-Call Teams

- Isolate the infected device
- Notify the SOC/IR Team
- Take a system snapshot or image
- Collect ransom note / IOCs
- Communicate with leadership
- Begin containment and eradication
- Document everything